JOURNAL OF NUMBER THEORY 40, 86–91 (1992)

On the Diophantine Equation $x^2 - Dy^2 = nz^2$

EDWARD L. COHEN

Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5

Communicated by N. C. Ankeny

Received March 15, 1988

Certain diophantine equations of the form $x^2 - Dy^2 = nz^2$ are solved parametrically. In particular, a case where $D = -11$ and $n = 3$ is studied in detail. Several examples show the utilization of quadratic forms in equations of this kind.

1. INTRODUCTION

Let $E := |D|$. If E is prime (or 1) and D is of the form $\sigma^2(r) - n\tau^2(r)$, where $\sigma(r)$ and $\tau(r)$ are linear, then it is possible to find all the solutions of the diophantine equation

$$x^2 - Dy^2 = nz^2 \qquad (xyz \neq 0) \tag{1}$$

parametrically. We take n as prime also and explain in Section 4 why n and E are so chosen. In general, the equation $ax^2 + by^2 + cz^2 = 0$ has been studied in recent times by many authors (see, e.g., [1–4]) in various ways and goes back to the time of Euler.

2. EXAMPLES OF EQ. (1)

The following D (many more of which can be obtained) give examples of Eq. (1):

(α) $D = 2r^2 - 1 = (2r+1)^2 - 2(r+1)^2$

(β) $D = 2 - 9r^2 = (3r+2)^2 - 2(3r+1)^2$

(γ) $D = r^2 - 2r - 1 = (3r+1)^2 - 2(2r+1)^2$

(δ) $D = 1 - 3r^2 = (3r+2)^2 - 3(2r+1)^2$.

Thus (α), (β), and (γ) are of the form $x^2 - Dy^2 = 2z^2$, while (δ) is of the form $x^2 - Dy^2 = 3z^2$.

0022-314X/92 $3.00

3. Parametric Solutions to Eq. (1)

First, we solve the general equation (1) and then specialize to particular examples. Note that for every positive integer n and every positive integer E, prime or not, of the form $|\sigma^2(r) - n\tau^2(r)|$, Eq. (1) possesses a solution; namely, $x = \sigma(r)$, $y = 1$, $z = \tau(r)$.

Let x, y, z be integer solutions of Eq. (1). From (1), we obtain

$$(x + \sigma(r)\, y)(x - \sigma(r)\, y) = n(z + \tau(r)\, y)(z - \tau(r)\, y).$$

This gives essentially two classifications (all the rest give the same results). The first classification is

$$\begin{aligned} x - \sigma(r)\, y &= M(z + \tau(r)\, y) \\ M(x + \sigma(r)\, y) &= n(z - \tau(r)\, y), \end{aligned} \tag{2}$$

where we can take M to be an *arbitrary* reduced rational. Rewriting Eqs. (2) into parametric form, we obtain

$$\frac{x}{\sigma(r)M^2 + 2n\tau(r)M + n\sigma(r)} = \frac{y}{n - M^2} = \frac{z}{\tau(r)M^2 + 2\sigma(r)M + n\tau(r)}.$$

Write $M = u/v$ with $\gcd(u, v) = 1$, $v > 0$ and let

$$\begin{aligned} e &= \sigma(r)u^2 + 2n\tau(r)uv + n\sigma(r)v^2 \\ f &= nv^2 - u^2 \\ g &= \tau(r)u^2 + 2\sigma(r)uv + n\tau(r)v^2. \end{aligned} \tag{3}$$

The second classification is

$$\begin{aligned} x - \sigma(r)\, y &= M(z - \tau(r)\, y) \\ M(x + \sigma(r)\, y) &= n(z + \tau(r)\, y) \end{aligned} \tag{4}$$

and rewriting Eqs. (4) we obtain

$$\frac{x}{\sigma(r)M^2 - 2n\tau(r)M + n\sigma(r)} = \frac{y}{n - M^2} = \frac{z}{-\tau(r)M^2 + 2\sigma(r)M - n\tau(r)},$$

giving

$$\begin{aligned} e &= \sigma(r)u^2 - 2n\tau(r)uv + n\sigma(r)v^2 \\ f &= nv^2 - u^2 \\ g &= -\tau(r)u^2 + 2\sigma(r)uv - n\tau(r)v^2. \end{aligned} \tag{5}$$

From both of these classifications the form $x/e = y/f = z/g$ is derived.

Let $h = \gcd(e, f, g)$. The greatest common divisor h of e, f, g divides

$$\sigma(r)e \mp n\tau(r)g = D(u^2 + nv^2).$$

Also h divides $f = nv^2 - u^2$. Now $\gcd(u^2 + nv^2, nv^2 - u^2) = 1$, 2, or n. Thus it follows that $h \mid 2nE$. Therefore, $h = 1$, n, E, nE, 2, $2n$, $2E$, or $2nE$. [Since D may be ± 1 or ± 2 and n may be 1 or 2, we do not necessarily obtain eight gcd's. The outcome of this is stated in Section 4 because of its importance.]

Once can verify that *every* triple

$$(x, y, z) = \left(\frac{ce}{h}, \frac{cf}{h}, \frac{cg}{h}\right) \tag{6}$$

is a solution of (1); therefore, Eq. (1) is equivalent to system (6) when the two classifications are used. For $c = \pm 1$, we obtain the primitive solutions of (1).

4. The General Cases of Eq. (1)

We break up Eq. (1) into the following all-encompassing cases and consider in Sections 5 and 6 examples of cases (i), (iii), and especially (iv):

(i) $|D| = 1$ or 2, $n = 1$ or $2 \Rightarrow h = 1$ or 2

(ii) $|D| = 1$ or 2, $n > 2 \Rightarrow h = 1$, 2, n, or $2n$

(iii) $|D| > 2$, $n = 1$ or $2 \Rightarrow h = 1$, 2, E, or $2E$

(iv) $|D| > 2$, $n > 2 \Rightarrow h = 1$, 2, E, $2E$, n, $2n$, nE, or $2nE$.

Remark. As noted in Section 1, we observe that E and n need not be prime; however, the large number of gcd's possible would make the task more difficult.

5. Particular Examples of Eq. (1)

Example 1. Case (i), with E and $n = 1$ in Section 4, gives rise to the Pythagorean triples with $e = u^2 + v^2$, $f = v^2 - u^2$, $g = 2uv$. Here, $\sigma(r) = \pm 1$ and $\tau(r) = 0$. The two classifications give exactly the same results.

Example 2. For another example of Eq. (1), see [1], where case (iii) and the first classification are discussed for $D = 7$ and $n = 2$, this case arising from (α) with $r = 2$.

EXAMPLE 3. We now work out a particular example of case (iv), namely, the case of (δ), which was noted in Section 2.

In general, let $E = |D| > 2$, $n > 2$. Obviously this case is the most complicated. We state two lemmas that can easily be proven.

LEMMA 1. $n \mid u \Leftrightarrow n \mid \gcd(e, f, g) \Leftrightarrow n \mid n$, nE, $2n$, *or*, $2nE$.
This can be verified by Eqs. (3) *and* (5). *Again by these equations we observe the following if n is odd*:

LEMMA 2. (a) *u and v are of opposite parity* $\Leftrightarrow h = 1$, E, n, *or* nE.
(b) *u and v are of the same parity* $\Leftrightarrow h = 2$, $2E$, $2n$, *or* $2nE$.

Now let $D = 1 - 3r^2 = (3r+2)^2 - 3(2r+1)^2$. Suppose $n = 3$ does not divide u. Define $H := E$ if u and v are of opposite parity; otherwise, $H := 2E$ if u and v are of the same parity.

PROPOSITION A (First Classification). $H = \gcd(e, f, g) \Leftrightarrow u \equiv -3rv \pmod{E}$.

Proof. ($\Rightarrow$) By (3),

$$\begin{aligned} (3r+2)u^2 + 6(2r+1)uv + 3(3r+2)v^2 &\equiv 0 \pmod{E} \\ 3v^2 - u^2 &\equiv 0 \pmod{E}. \end{aligned} \tag{7}$$

Hence,

$$(3r+2)u + 3(2r+1)v \equiv 0 \pmod{E}. \tag{8}$$

Multiplying (8) by $(2-3r)$ yields $u + 3rv \equiv 0 \pmod{E}$.

($\Leftarrow$) Let $u + 3rv \equiv 0 \pmod{E}$. We need only show that (7) and (8) hold. Since $(3r+2)(2-3r) \equiv 1 \pmod{E}$, (8) follows by dividing $u + 3rv$ by $2 - 3r$ [or multiplying by $3r + 2$]. For the second part of (7), note that $u \equiv -3rv \pmod{E} \Rightarrow u^2 \equiv 9r^2v^2 \pmod{E}$. Because $9r^2 - 3 \equiv 0 \pmod{E}$, we observe that $u^2 \equiv 3v^2 \pmod{E}$. With the facts we have just established it is now easy to verify the first part of (7).

COROLLARY A. $H = \gcd(e, f, g) \Leftrightarrow v \equiv -ru \pmod{E}$. [*Multiply through by r.*] *Note in the proposition and the corollary that if* $n \mid u$, *then* $\gcd(e, f, g) = nH$. (*The same applies in the next two results.*)

PROPOSITION B (Second Classification). $H = \gcd(e, f, g) \Leftrightarrow u \equiv 3rv \pmod{E}$.

COROLLARY B. $H = \gcd(e, f, g) \Leftrightarrow v \equiv ru \pmod{E}$.

Remark. For each Eq. (1) with D fixed and for each classification, there is an infinite number of solutions. Each primitive solution (x, y, z) is realized from rationals $M = u/v$ with $\gcd(u, v) = 1$. These u, v in case (iv) give rise to the *eight* gcd's of e, f, g.

6. An Example of (δ) with $r = 2$

Example 4. In Example 3, let $r = 2$ or $D = -11$ in (δ). Note that $n = 3$. Without loss of generality we can let $\gcd(u, v) = 1$. Equation (1) becomes $x^2 + 11y^2 = 3z^2$. The propositions with $\gcd(u, v) = 1$ give the following:

First classification

v	u		e/h	f/h	g/h	gcd	$(\sigma e - n\tau g)/h$
1	5	(mod 11)	17	−1	10	$2E$	−14
2	21	(mod 22)	148	−13	89	nE	−151
3	4	(mod 11)	64	1	37	E	−43
4	9	(mod 22)	64	−1	37	nE	−43
5	3	(mod 11)	17	1	10	$2nE$	−14
6	19	(mod 22)	652	−23	379	E	−469
7	2	(mod 11)	148	13	89	E	−151
8	7	(mod 22)	328	13	191	E	−241
9	1	(mod 11)	101	11	62	$2E$	−122
10	17	(mod 22)	892	1	515	E	−589
12	5	(mod 22)	496	37	295	E	−457

Note that $v = 11, 15, 21, 22, 24, 35, \ldots$ do not yield primitive solutions since $\gcd(u, v) \neq 1$.

Second classification

v	u		e/h	f/h	g/h	gcd	$(\sigma e - n\tau g)/h$
1	6	(mod 11)	4	−1	−3	nE	−13
2	1	(mod 22)	4	1	−3	E	−13
3	7	(mod 11)	−1	−1	−2	$2E$	−38
4	13	(mod 22)	16	−11	−23	E	−217
5	8	(mod 11)	−8	1	−5	E	−139
7	9	(mod 11)	−1	1	−2	$2nE$	−38
8	15	(mod 22)	−8	−1	−5	nE	−139
9	10	(mod 11)	4	13	−25	E	−343
12	17	(mod 22)	−32	13	−31	E	−721

Note that $v = 6, 10, 11, 14, 18, 22, \ldots$ do not yield primitive solutions since $\gcd(u, v) \neq 1$.

7. Further Examples

The results of integral quadratic forms used in this section can be found in Watson [5, Chap. 1, Section 4]. We deal with the first classification. Similar results can be obtained for the second classification.

Example 5. For the equation $x^2 - Dy^2 = nz^2$, let $A = \sigma(r)$, $B = \tau(r)$. Then the matrix M_e representing the quadratic form $e = \text{row}[(A, nB), (nB, nA)]$. Similarly, the matrix M_g representing the quadratic form $g = \text{row}[(B, A), (A, nB)]$. Let $T_{eg} = \text{row}[(0, 1), (1/n, 0)]$. A simple calculation will show that $M_e T_{eg} = M_g$.

Example 6. In case (γ), let $r = 4$. Then $D = 7$, $n = 2$, $A_\gamma = 13$, $B_\gamma = 9$. In case (α), let $r = 2$. Then $D = 7$, $n = 2$, $A_\alpha = 5$, $B_\alpha = 3$. So the equation for both is $x^2 - 7y^2 = 2n^2$. From quadratic forms, we obtain a one–one relationship between $M_{\gamma(e)}$ and $M_{\alpha(e)}$, also between $M_{\gamma(g)}$ and $M_{\alpha(g)}$. For particular matrices J and K, $M_{\gamma(e)} J = M_{\alpha(e)}$ and $M_{\gamma(g)} K = M_{\alpha(g)}$, with $\det J = \det K = 1$. The calculation gives $M_{\gamma(e)} = \text{row}[(13, 18), (18, 26)]$, $J = \frac{1}{7}\,\text{row}[(11, -12), (-6, 11)]$, $M_{\alpha(e)} = \text{row}[(5, 6), (6, 10)]$, $M_{\gamma(g)} = \text{row}[(9, 13), (13, 18)]$, $K = \frac{1}{7}\,\text{row}[(11, -12), (-6, 11)]$, $M_{\alpha(g)} = \text{row}[(3, 5), (5, 6)]$. Because $T_{\gamma(e)\gamma(g)} = T_{\alpha(e)\alpha(g)} \equiv T$, we also have the relation that $J = TKT^{-1}$, where T, in this case, is equal to $\text{row}[(0, 1), (\frac{1}{2}, 0)]$.

Example 7. We let the example of case (γ) be as in Example 6, and for (β), we take $r = 1$. Then, for our case of (β), $D = -7$, $n = 2$, $A_\beta = 5$, $B_\beta = 4$. The diophantine equation associated with (β) is $x^2 + 7y^2 = 2z^2$. There is a matrix L with $\det L = -1$ such that $M_{\gamma(e)} L = M_{\beta(e)}$. Here $L = \text{row}[(-1, 2), (1, -1)]$. Other relevant matrices with respect to these particular cases of (β) and (γ) can also be obtained.

References

1. E. L. Cohen, Equations of the form $x^2 - Dy^2 = 2z^2$, *Math. Student* **50** (1982), 106–110 (1987).
2. R. H. Hudson and K. S. Williams, On Legendre's equation $ax^2 + by^2 + cz^2 = 0$, *J. Number Theory* **16** (1983), 101–105. [MR84e:10022]
3. L. J. Mordell, Diophantine equations, *in* "Pure and Applied Mathematics," Vol. 30, Academic Press, London/New York, 1969. [MR40 #2600; Zbl. 188, 345]
4. Th. Skolem, On the diophantine equation $ax^2 + by^2 + cz^2 = 0$, *Univ. Roma 1st. Naz. Alta Mat. Appl.* **11** (5) (1952), 88–100. [MR15, 601i]
5. G. L. Watson, Integral quadratic forms, *in* "Cambridge Tracts in Mathematics and Mathematical Physics" Vol. 51, Cambridge Univ. Press, New York, 1960. [MR22 #9475]